UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/038,169	01/02/2002	Dan Boneh	36321-8009.US01	7811

22918 7590 06/01/2007

PERKINS COIE LLP
P.O. BOX 2168
MENLO PARK, CA 94026

EXAMINER	
TO, BAOTRAN N	

ART UNIT	PAPER NUMBER
2135	

MAIL DATE	DELIVERY MODE
06/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/038,169	BONEH ET AL.	
	Examiner	Art Unit	
	Baotran N. To	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *03/16/2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-3,5,7-24 and 26-31* is/are pending in the application.

4a) Of the above claim(s) *4, 6 and 25* is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5,7-13,18-24 and 28-31* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action is responsive to the Applicant's Amendment filed 03/16/2007.

Claims 1, 2, 18, 23, 28 and 29 are currently amended.

Claims 14-17 and 26-27 are previously withdrawn.

Claims 4, 6 and 25 are previously canceled.

Claims 1-3, 5, 7-24, 26-31 are pending in the application.

Response to Arguments

2. Applicant's arguments filed 03/16/2007 have been fully considered but they are not persuasive.

Applicant argues, "Although Korn discloses identifying and blocking sensitive data within the content using pre-defined sequences or patterns, it does not teach enabling a user to specify a which data fields are sensitive at his/her own discretion" (Page 1 of Remarks).

Examiner respectfully disagrees with this argument. Korn explicitly discloses, "The predefined sequences might be entered by a user and stored in a data file on a hard disk drive 11 (see FIG. 1) of the computer 10. When the computer 10 initializes the keyboard input program 14 for execution, the computer 10 may, for example, store an image of the data file as a memory mapped file in a memory of the computer 10" (col. 3, lines 35-40). Korn further discloses, "In some embodiments, the computer 10 (under control of the keyboard input program 14) may identify the personal information items by comparing the received sequence of keystroke data to predefined patterns, each of

which may indicate a different personal information item. For example, a credit card number may follow the pattern "XXXX-XXXX-XXXX-XXXX," where each "X" indicates a single digit number from zero to nine. In this manner, if a portion of the received keystroke sequence indicates the predefined pattern, then one of the personal information items is identified" (col. 3, lines 40-51).

Applicant further argues, "Neither Lewis nor Korn teach checking the received content before it reaches components in a server environment, which is important for protecting sensitive user data in the content from being exposed to unauthorized access. Moreover, neither Lewis nor Korn disclose encrypting data at a point between the client and the server." (Page 2 of Remarks).

Examiner respectfully disagrees with applicant. Korn explicitly discloses "Referring back to FIG. 1, the action taken by the computer 10 (after determining a stream to be transmitted indicates one or more personal information items) may include, in some embodiments, determining whether the browser application program 12 is using a secure protocol to transmit data. For example, in some embodiments, the computer 10 may automatically determine whether the browser application program 12 is causing the computer 10 to use an encryption protocol, such as a protocol used by a secure sockets layer (SSL), in communications with other computers. However, in other embodiments, instead of automatically making this determination, the computer 10 may prompt the user to indicate the type of protocol being used by the browser application program 12. If the browser application program 12 is causing the computer 10 to transmit the data using a secure protocol, then, in some embodiments, the computer 10

may allow the data indicating personal information items to be transmitted to the computer 8. However, in other embodiments, even if the browser application program 12 is causing the computer 10 to transmit data using a secure protocol, the computer 10 may take steps to prevent the transmission of the data that indicates the personal information items" (col. 2, lines 26-48).

Applicant further discloses, "It follows that neither Lewis nor Korn disclose using a regular expression for selecting sensitive data in this manner" (Page 2 of Remarks).

Examiner respectfully disagrees with this contention. Korn explicitly discloses "In some embodiments, the computer 10 (under control of the keyboard input program 14) may identify the personal information items by comparing the received sequence of keystroke data to predefined patterns, each of which may indicate a different personal information item. For example, a credit card number may follow the pattern "XXXX-XXXX-XXXX-XXXX," where each "X" indicates a single digit number from zero to nine. In this manner, if a portion of the received keystroke sequence indicates the predefined pattern, then one of the personal information items is identified" (col. 3, lines 40-51).

For at least the above reasons, it is believed that the rejection is maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claims 1-3, 5, 8-13, 18-24 and 28-31 are rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis et al. (U.S. Patent 6,233,565 B1) herein referred to as Lewis in view of Korn et al. (U.S. Patent 6,442,607 B1) herein referred to as Korn.

Regarding Claims 1 and 28, Lewis discloses a system for protecting sensitive information residing in server environments, comprising at least one processing device coupled among at least one network and at least one client computer (col. 2, lines 30-33), wherein the at least one processing device (server):

receives at least one electronic transaction query (transaction request) from the at least one client computer (client) via at least one secure channel (SSL) (col. 5, lines 30-40 and col. 15, lines 40-45);

encrypts the specified sensitive data (col. 14, lines 26-28);

transfers the encrypted sensitive data among components of the server environment (col. 29, lines 27-34);

receives at least one electronic information query for the encrypted sensitive data from at least one third-party system via the at least one secure channel (col. 14, lines 25-29);

decrypts the encrypted sensitive data in response to the at least one electronic information query (col. 16, lines 65-67); and

provides the decrypted sensitive data to the at least one third-party system via the at least one secure coupling (private network connection) (col. 17, lines 1-5).

Lewis does not discloses "enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment."

However, Korn expressly discloses enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment (Figure 2, col. 2, lines 4-20, col. 3, lines 20-64).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Korn's invention with Lewis to include enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment. One of ordinary skill in the art would have been motivated to prevent the transmission of the data that indicates the personal information items (Korn, col. 2 lines 47-48).

Regarding Claim 2, Lewis discloses a method for protecting sensitive information within server environments, comprising:

wherein sensitive data of the at least one electronic request is encrypted before transfer among components of the server environment (col. 14, lines 25-30)

wherein encrypted sensitive data of the server environment is decrypted before transfer from the server environment (col. 17, lines 1-3).

Lewis does not discloses "enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment."

However, Korn expressly discloses enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment (Figure 2, col. 2, lines 4-20, col. 3, lines 20-64).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Korn's invention with Lewis to include enables a user to specify, via regular expression, a plurality of fields of sensitive data to be encrypted within the at least on electronic transaction query before it reaches components in the server environment. One of ordinary skill in the art would have been motivated to prevent the transmission of the data that indicates the personal information items (Korn, col. 2 lines 47-48).

Regarding Claim 3, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses comprising determining that the at least one electronic request includes sensitive data (col. 14, lines 35-40).

Regarding Claim 5, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses determining that sensitive data in the electronic request

includes at least one user password; and applying at least one hash function to the at least one user password (col. 22, lines 58-63).

Regarding Claim 8, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one electronic request comprises at least one protocol over Secure Socket Layer (col. 15, col. 40-45).

Regarding Claims 9 and 21, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the sensitive data comprises at least one data item selected from a group including credit card numbers, credit card information, account numbers, account information, birth dates, social security numbers, user information, and user passwords (col. 17, lines 5-15).

Regarding Claim 10, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses executing the at least one cryptographic operation using at least one public key (col. 22, lines 20-25).

Regarding Claims 11 and 22, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one cryptographic operation includes at least one operation selected from a group including encryption operations, decryption operations, hash operations, keyed hash operations, and keyed hash verification (col. 22, lines 60-65).

Regarding Claim 12, Lewis and Korn disclose the limitations as discussed in Claims 2, above. Lewis further discloses wherein encrypting includes performing at least one operation on the sensitive data selected from a group including hashing and keyed hashing when the sensitive data is a password (col. 22, lines 58-64).

Regarding Claim 13, Lewis and Korn disclose the limitations as discussed in Claim 2 above. Lewis further discloses wherein the at least one electronic request comprises at least one encoded key identifier (col. 23, lines 25-35).

Regarding Claim 18, Lewis discloses a system for protecting sensitive information within server systems, comprising

at least one processing device coupled among at least one server site and at least one client computer and at least one network (FIG. 2, col. 5, lines 30-40 and col. 15, col. 40-45),

wherein the at least one processing device applies at least one cryptographic operation to sensitive data in response to the at least one electronic request (col. 14, lines 25-28),

wherein the sensitive data of the at least one electronic request is encrypted prior to transfer among components of the at least one server system (col. 14, lines 26-28),

wherein encrypted sensitive data of the at least one server system is decrypted prior to transfer among the at least one network (col. 17, lines 1-3).

Lewis does not disclose "wherein the at least one processing device enables a user to specify, using regular expression, sensitive data to be encrypted inside the electronic request before it reaches components of at least one server system."

However, Korn expressly discloses wherein the at least one processing device enables a user to specify, using regular expression, sensitive data to be encrypted inside the electronic request before it reaches components of at least one server system (Figure 2, col. 2, lines 4-20, col. 3, lines 20-64).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Korn's invention with Lewis to include wherein the at least one processing device enables a user to specify, using regular expression, sensitive data to be encrypted inside the electronic request before it reaches components of at least one server system. One of ordinary skill in the art would have been motivated to prevent the transmission of the data that indicates the personal information items (Korn, col. 2 lines 47-48).

Regarding Claim 19, Lewis and Korn disclose the limitations as discussed in Claim 18 above. Lewis further discloses wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags indicating that associated data is the sensitive data (col. 6, lines 1-15).

Regarding Claim 20, Lewis and Korn disclose the limitations as discussed in Claim 18 above. Lewis further discloses wherein the at least one processing device determines that the at least one electronic request includes sensitive data by identifying tags specified by at least one system administrator that associated data is the sensitive data (col. 6, lines 1-15).

Regarding Claim 23, Lewis discloses a cryptographic appliance for securing sensitive information within a server system, comprising:

at least one processing device coupled among at least one server system and at least one network coupling to evaluate at least one received electronic request in a first protocol format (col. 5, lines 30-40 and col. 15, lines 40-45),

wherein the at least one processing device (server) (FIG. 2);

encrypts the sensitive data (col. 14, lines 26-28).

Lewis explicitly does not disclose "enables a user to specify, via regular expression, sensitive data to be encrypted in the at least received electronic request before it reaches components of at least one the server system."

However, Korn expressly discloses enables a user to specify, via regular expression, sensitive data to be encrypted in the at least received electronic request before it reaches components of at least one the server system (Figure 2, col. 2, lines 4-20, col. 3, lines 20-64).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Korn's invention with Lewis to include

enables a user to specify, via regular expression, sensitive data to be encrypted in the at least received electronic request before it reaches components of at least one the server system. One of ordinary skill in the art would have been motivated to prevent the transmission of the data that indicates the personal information items (Korn, col. 2 lines 47-48).

Lewis and Korn disclose the limitations as discussed in Claim 23 above. Lewis further discloses reforms the electronic request, including the encrypted sensitive data, in the first protocol format (Korn, col. 3, lines 20-64); transfers the reformed electronic request among at least one component of the at least one server system (col. 29, lines 27-34).

Regarding Claim 24, Lewis and Korn disclose the limitations as discussed in Claim 23 above. Lewis further discloses wherein the at least one processing device:

evaluates at least one request for the encrypted sensitive data received via at least one coupling with at least one third-party system (col. 2, lines 30-40);

decrypts the encrypted sensitive data (col. 14, lines 26-28); and

transfers the decrypted sensitive data to the at least one third-party system (col. 17, lines 1-5).

Regarding Claim 29, Lewis a device comprising:

a processor (Figure 2);

a network interface coupled to the processor (Figure 2);

a pattern specification engine coupled to the processor (Figure 2);

a cryptographic engine coupled to the processor (Figure 2);

wherein, in operation, first one or more packets including payload formatted in a first protocol are input on the network interface (col. 5, lines 30-40 and col. 15, lines 40-45);

the cryptographic engine applies a cryptographic transformation to the sensitive data (col. 29, lines 27-34);

the processor forms second one or more packets including the cryptographically transformed sensitive data and the non-sensitive data in the first protocol (col. 14, lines 25-28);

the second one or more packets are output on the network interface (col. 29, lines 27-34);

Lewis explicitly does not disclose "the specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches components of a server environment."

However, Korn expressly discloses the specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches components of a server environment (Figure 2, col. 2, lines 4-20, col. 3, lines 20-64).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Korn's invention with Lewis to include the specification matching engine enables a user to apply a regular expression to the payload to specify which portion of the payload includes sensitive data to be encrypted and which portion of the payload includes non-sensitive data before the payload reaches components of a server environment. One of ordinary skill in the art would have been motivated to prevent the transmission of the data that indicates the personal information items (Korn, col. 2 lines 47-48).

Regarding Claim 30, Lewis and Korn disclose the limitations as discussed in Claim 29 above. Lewis further discloses a database of cryptographic keys, wherein, in operation, the cryptographic engine uses a key from the database of cryptographic keys to cryptographically transform the sensitive data (col.22, lines 1-50).

Regarding Claim 31, Lewis and Korn disclose the limitations as discussed in Claim 29 above. Lewis further discloses wherein the cryptographic transformation includes decryption or encryption (col. 29, lines 26-35).

4. Claim 7 is rejected under 35 U.S.C. 103(a) as being unpatentable over Lewis and Korn as applied to claim 2 above, and further in view of Devine et al. (U.S. Patent 6,598,167 B2) herein referred to as Devine.

Regarding Claim 7, Lewis and Korn disclose the limitations as discussed in Claim 2 above.

Lewis and Korn explicitly does not disclose "determining the at least one electronic request includes one or more cookies; identify at least one cookie of the one or more cookies that includes sensitive data; applying at least one cryptographic function or checksum to the at least one cookie."

However, Devine teaches "determining the at least one electronic request includes one or more cookies; identify at least one cookie of the one or more cookies that includes sensitive data; applying at least one cryptographic function or checksum to the at least one cookie" (col. 8, lines 45-60).

Therefore, It would have been obvious to one of ordinary skill in the art at the time the invention was made to incorporate Devine's invention with Lewis and Korn to have included the cookie with the motivation being to allow adding an additional level of security (col. 8 lines 55-60).

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BT
05/24/2007

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100